

*В. С. Пустовит*¹✉

Метод формирования виртуальных защищенных каналов связи с использованием российских криптографических алгоритмов

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: VSPustovit@mephi.ru

Аннотация. В статье рассматривается метод построения виртуальных защищенных каналов связи (ВЗКС), полностью базирующийся на российских криптографических стандартах. Актуальность работы обусловлена законодательными требованиями по импортозамещению в области защиты информации и выявленными в ходе сравнительного анализа недостатками популярных решений (OpenVPN, WireGuard, L2TP/IPsec), связанными с использованием зарубежных криптографических алгоритмов. Целью исследования является разработка метода формирования ВЗКС, обеспечивающих конфиденциальность сетевого взаимодействия на базе стека TCP/IPv4 с применением российских криптографических алгоритмов. В основу предложенного метода положена адаптация паттерна IK фреймворка Noise Protocol, реализованная на алгоритмах VKO (ГОСТ Р 50.1.113-2016), шифрования «Кузнечик» в режиме MGM (ГОСТ Р 34.12/13-2018) и хэширования «Стрибог» (ГОСТ Р 34.11-2018). Предложенный метод позволяет достичь минимальной задержки установления соединения (1-RTT с возможностью 0-RTT шифрования данных). В работе представлена модульная архитектура децентрализованной системы с сервером для управления узлами и прямого P2P-туннелирования трафика. Результатом работы является формализованное описание криптографического рукопожатия на основе паттерна IK, структур пакетов взаимодействия и диаграммы состояний туннеля, что в совокупности образует законченную спецификацию метода и создаёт основу для практической реализации сертифицируемого средства защиты информации.

Ключевые слова: виртуальный защищенный канал связи, российские криптографические алгоритмы, децентрализованная архитектура

*V. S. Pustovit*¹✉

Establishing secure virtual communication channels method using russian cryptographic algorithms

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: VSPustovit@mephi.ru

Abstract. This article discusses a method for establishing virtual secure communication channels (VSCCs) based entirely on Russian cryptographic standards. The relevance of this work stems from legislative requirements for import substitution in the field of information security and the shortcomings of popular solutions (OpenVPN, WireGuard, L2TP/IPsec) identified during a comparative analysis, which are related to the use of foreign cryptographic algorithms. The aim of the research is to develop a method for creating VSCs that ensure the confidentiality of network interactions based on the TCP/IPv4 stack using Russian cryptographic algorithms. The proposed method is based on an adaptation of the IK pattern of the Noise Protocol framework, implemented using VKO algorithms (GOST R 50.1. 113-2016), the “Kuznechik” cipher in MGM mode (GOST R 34.12/13-2018), and the “Stribog” hash function (GOST R 34.11-2018). The proposed method allows for minimal connection establishment delay (1-RTT with the possibility of 0-RTT data encryption). The paper pre-

sents a modular architecture of a decentralized system with a server for node management and direct P2P traffic tunneling. The result of this work is a formalized description of a cryptographic handshake based on the IK pattern, interaction packet structures, and a tunnel state diagram, which together form a complete specification of the method and provide the foundation for the practical implementation of a certifiable information security solution.

Keywords: secure virtual communication channel, Russian cryptographic algorithms, decentralized architecture

Введение

Рост популярности удалённой и гибридной занятости, а также необходимость объединения территориально распределённых филиалов в единое информационное пространство сопровождаются увеличением объёмов данных, передаваемых через публичные сети. В этих условиях обеспечение конфиденциальности и целостности сетевого взаимодействия становится критически важной задачей, решаемой посредством виртуальных защищённых каналов связи (ВЗКС). Нормативно-правовая база Российской Федерации [1–7] (ФЗ № 187, ФЗ № 152, Приказ ФСБ № 66) прямо предписывает применение сертифицированных российских криптографических средств для защиты информации ограниченного доступа.

Широко распространённые технологии построения ВЗКС, такие как OpenVPN, WireGuard и L2TP/IPsec, обладают рядом принципиальных ограничений. Проведённый сравнительный анализ показал, что OpenVPN и L2TP/IPsec ориентированы на зарубежные криптографические примитивы (AES, RSA) и демонстрируют значительное падение пропускной способности (до 97%) [8–10]. WireGuard, несмотря на высокую производительность, использует фиксированный стек алгоритмов (ChaCha20, Curve25519) [11–13] и не поддерживает отечественные стандарты ГОСТ, что исключает его применение в аттестуемых системах. Кроме того, все три протокола обладают устойчивыми сигнатурами, позволяющими обнаруживать и блокировать их трафик с помощью средств глубокого анализа пакетов.

Существующие научные подходы к совершенствованию ВЗКС либо ориентированы на нейросетевую аутентификацию без строгого криптографического обоснования [14–16], либо опираются на аппаратно-зависимые квантовые технологии [17–19]. В патентных решениях (RU2820803C1, RU2838158C1) преобладают централизованные архитектуры с двойной инкапсуляцией, что приводит к избыточным задержкам и усложнению управления. Таким образом, актуальность настоящего исследования обусловлена отсутствием легковесного метода построения ВЗКС, одновременно удовлетворяющего требованиям российских регуляторов по применению ГОСТ, обладающего высокой пропускной способностью и устойчивого к пассивному обнаружению трафика.

Целью исследования является разработка метода построения виртуальных защищённых каналов связи на основе российских криптографических алгоритмов, обеспечивающей конфиденциальность сетевого взаимодействия при использовании стека протоколов TCP/IP версии 4.

Предлагаемое решение

Для обоснования необходимости разработки нового метода был проведён экспериментальный сравнительный анализ трёх наиболее распространённых технологий построения ВЗКС: OpenVPN (в конфигурации UDP/TLS), WireGuard и L2TP/IPsec. Исследование выполнялось в виртуальной сетевой лаборатории под управлением гипервизора Proxmox VE 9.0.3 на базе ОС Ubuntu Server 24.04. Измерения производились по 16 количественным и качественным критериям, включая пропускную способность, задержку установления соединения, накладные расходы на инкапсуляцию, а также поддержку отечественных криптоалгоритмов.

Проведённый сравнительный анализ существующих решений показал следующее. WireGuard демонстрирует наилучшую производительность (установка соединения <10 мс, падение скорости <20%) за счёт работы на уровне ядра, однако использует фиксированный набор зарубежных криптоалгоритмов и не соответствует требованиям ГОСТ, что исключает его сертификацию. OpenVPN, напротив, обладает гибкостью в выборе криптографии, но работает в пользовательском пространстве, что приводит к падению пропускной способности до 97% и высокой нагрузке на процессор [20]. L2TP/IPsec характеризуется наихудшими показателями из-за двойной инкапсуляции и опоры на устаревшие алгоритмы. Кроме того, трафик всех трёх протоколов устойчиво идентифицируется средствами DPI. Таким образом, ни одно из рассмотренных решений не сочетает соответствие российским криптографическим стандартам с высокой производительностью и устойчивостью к пассивному обнаружению.

В основу предлагаемого метода положена адаптация паттерна ИК фреймворка Noise Protocol Framework [21], обеспечивающая минимальное количество раундов взаимодействия при установлении защищённого соединения. Выбор паттерна ИК обусловлен возможностью выполнения рукопожатия за 1-RTT с опциональной поддержкой 0-RTT шифрования данных, что существенно сокращает задержку начала полезной передачи. Также предлагается отойти от традиционного клиент-серверного взаимодействия в пользу децентрализованной архитектуры, включающей сервер управления узлами и равноправные P2P-узлы, что повышает масштабируемость и отказоустойчивость системы.

Криптографическое ядро метода полностью опирается на российские стандарты. Генерация ключевых пар выполняется по ГОСТ Р 34.10-2018, согласование ключей — по протоколу VKO (ГОСТ Р 50.1.113-2016), симметричное шифрование — алгоритмом «Кузнечик» в режиме аутентифицированного шифрования MGM (ГОСТ Р 34.12/13-2018), хэширование и диверсификация ключей — функцией «Стрибог» (ГОСТ Р 34.11-2018) в составе HKDF.

Процедура формирования ВЗКС можно разбить на 7 фаз, начиная с регистрации узла, заканчивая передачей данных внутри. Данная процедура представлена в виде UML-диаграммы последовательности (рис. 1–3).

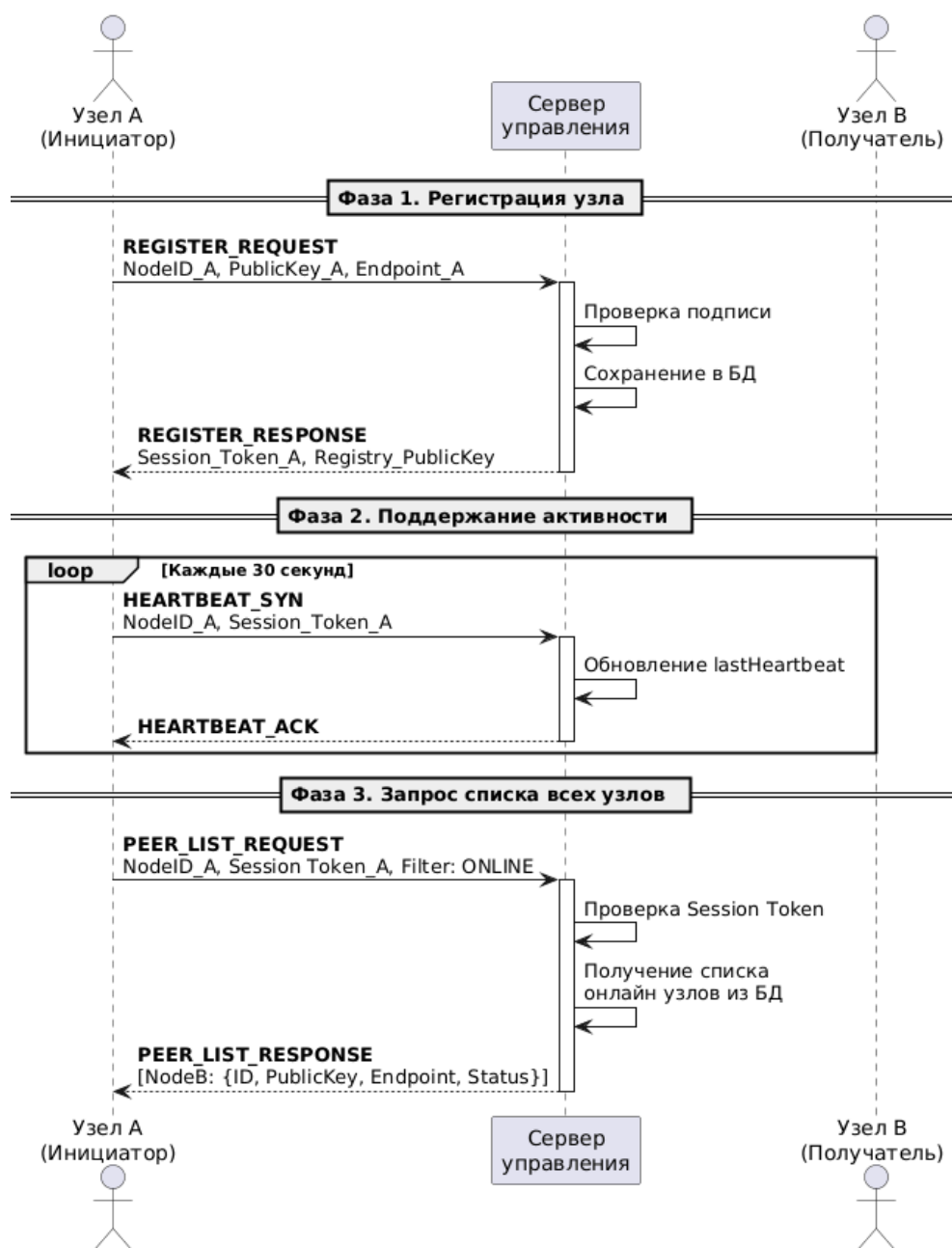


Рис. 1. UML-диаграмма последовательности формирования ВЗКС (фазы 1-3)

Прежде чем узел будет подключаться к другому узлу ему необходимо зарегистрировать себя в специальном сервере управления узлами. Его задача аутентифицировать каждый узел в сети и разрешать им соединяться прямыми P2P-соединениями.

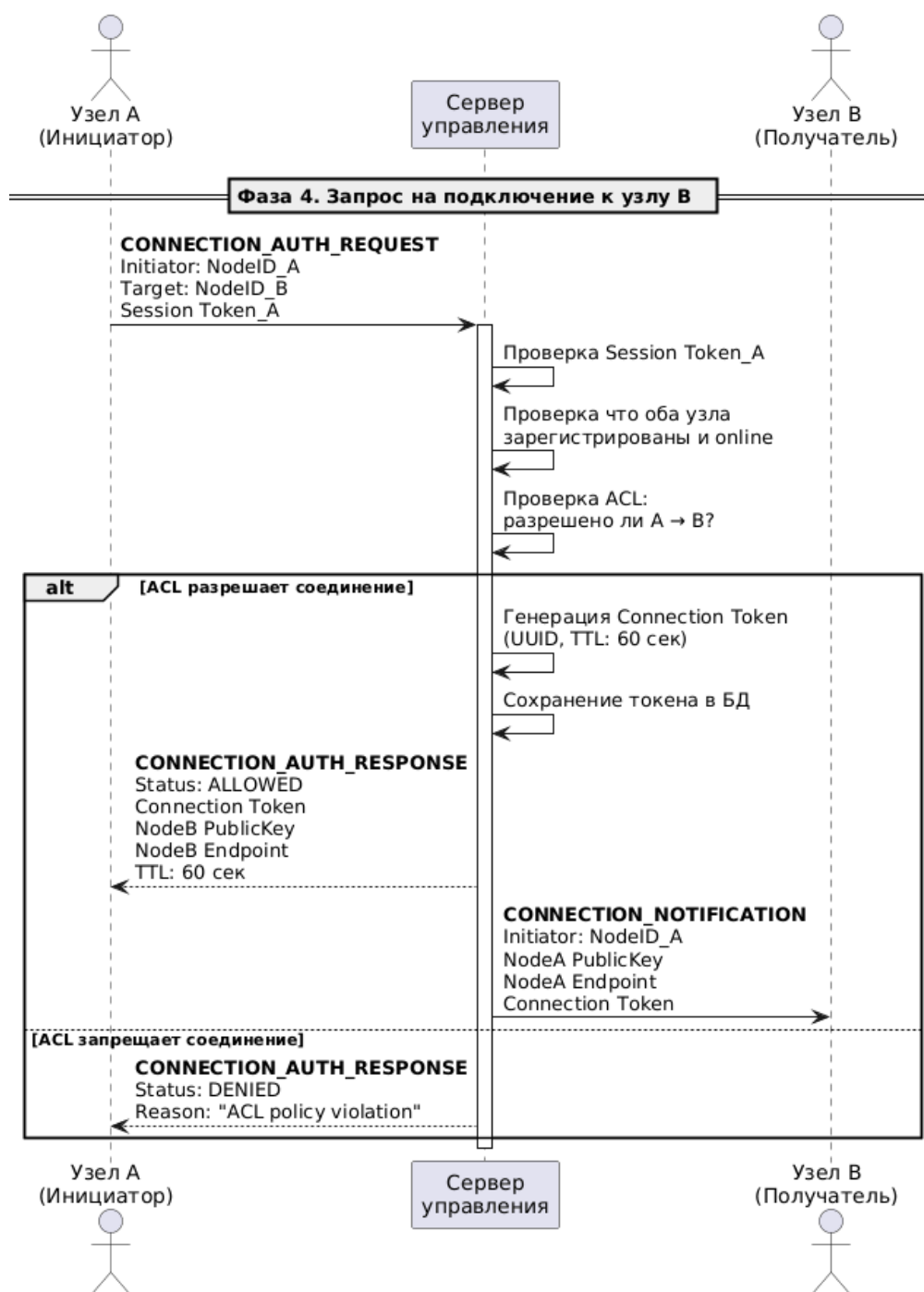


Рис. 2. UML-диаграмма последовательности формирования ВЗКС(фаза 4)

После регистрации и получения списка узлов в сети, инициатор может запросить доступ на подключение. Роль сервера управления разрешать и блокировать соединение двух узлов и при разрешении выдавать актуальную информацию о подключении (публичный статический ключ, адрес и порт подключения), а также уведомления второго узла, что к нему будут подключаться.

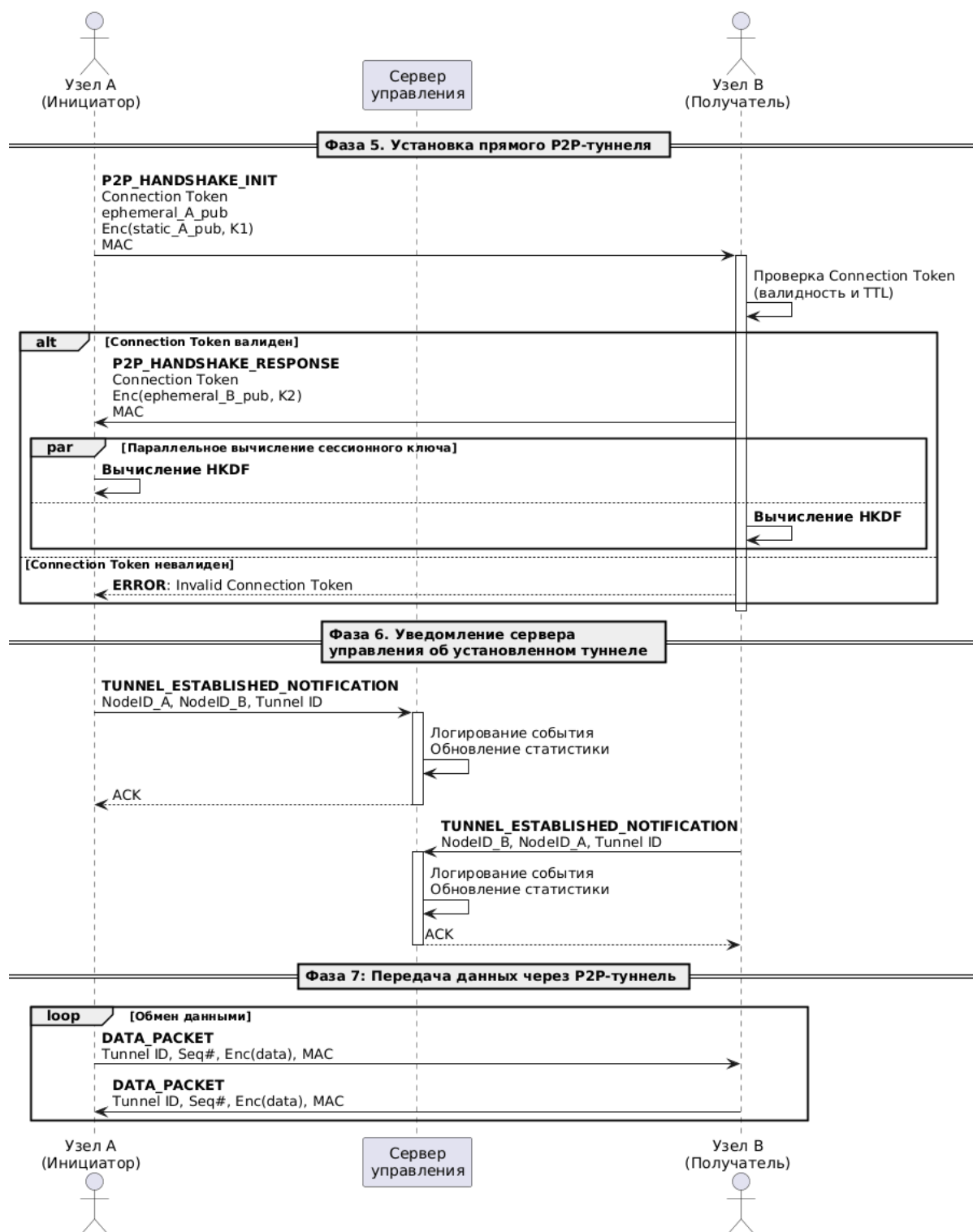


Рис. 3. UML-диаграмма последовательности формирования ВЗКС (фаза 5-7)

Если от сервера было разрешено соединение, то в разрешенное временное окно по ИК-паттерну Noise Protocol Framework происходит выработка сессионного ключа. Если все прошло успешно, оба узла сообщают серверу, что установлено соединение.

Заключение

В работе разработан метод формирования виртуальных защищённых каналов связи, основанный на адаптации паттерна ИК фреймворка Noise Protocol к российским криптографическим стандартам. Предложена формальная процедура установления защищённого соединения, включающая фазы регистрации узла, авторизации подключения, двухэтапного рукопожатия и защищённой передачи данных. Сформулировано описание криптографического ядра метода с использованием алгоритмов VKO для согласования ключей, шифра «Кузнечик» в режиме MGM для аутентифицированного шифрования и хэш-функции «Стрибог» для диверсификации ключей. Разработана процедура выработки сессионного ключа на основе четырёх комбинаций статических и эфемерных ключей, обеспечивающая свойство прямой секретности и завершающаяся за 1-RTT. Метод представлен в виде UML-диаграмм последовательности с детализацией по фазам и описанием структур передаваемых пакетов.

Метод ориентирован на построение отечественных средств защиты сетевого взаимодействия и может служить основой для программной реализации протокола с последующей сертификацией по требованиям ФСТЭК и ФСБ России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации "О Стратегии национальной безопасности Российской Федерации" от 02.07.2021 № 400 // Официальный интернет-портал правовой информации. – 2021;
2. Указ Президента Российской Федерации "Об утверждении Доктрины информационной безопасности Российской Федерации" от 05.12.2016 № 646 // Официальный интернет-портал правовой информации. – 2016;
3. Указ Президента Российской Федерации "Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации" от 07.05.2018 № 899 // Официальный интернет-портал правовой информации. – 2018;
4. Указ Президента Российской Федерации "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" от 30.03.2022 № 166 // Официальный интернет-портал правовой информации. – 2022;
5. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ // Официальный интернет-портал правовой информации. – 2017 - Ст. 17-20;
6. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ // Официальный интернет-портал правовой информации. - 2006 г. - Ст. 19;
7. Приказ ФСБ РФ "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" от 09.02.2005 № 66 // Официальный интернет-портал правовой информации. - 2006 г. - с изм. и допол. в ред. от 12.04.2010;
8. IBM Cost of a Data Breach Report // IBM URL: <https://www.ibm.com/reports/data-breach>;

9. Verizon Data Breach Investigations Report // Verizon URL: <https://www.verizon.com/business/resources/reports/dbir>;
10. Data records breached worldwide // Statista URL: <https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/>;
11. WireGuard: Next Generation Kernel Network Tunnel // WireGuard URL: <https://www.wireguard.com/papers/wireguard.pdf>;
12. A Cryptographic Analysis of the WireGuard Protocol // Cryptology ePrint Archive URL: <https://ia.cr/2018/080>;
13. Master, Alexander and Garman, Christina, "A WireGuard Exploration" (2021). CERIAS Technical Reports. Paper 1. <http://dx.doi.org/10.5703/1288284317610>;
14. Zaenchkovski, A., Lazarev, A., Tukaev, D., & Epifanov V. (2022). Intelligent information flow management system in innovative scientific and industrial clusters. International Journal of Parallel, Emergent and Distributed Systems, 37(3), 303–317. <https://doi.org/10.1080/17445760.2022.2060976>;
15. Artur Zaenchkovski, Alexey Lazarev. Development of an intelligent decision-making system to support scientific and industrial formations VPN connections. E3S Web Conf. 431 05034 (2023). DOI: 10.1051/e3sconf/202343105034;
16. Заенчковский А. Э., Лазарев А. И., Леднева О. В., Прокимнов Н. Н. Анализ и тестирование алгоритмов нейросетевой TCP/IP маршрутизации пакетов в частных виртуальных туннелях // Прикладная информатика. 2023. Т. 18. № 6. С. 98–108. DOI: 10.37791/2687-0649-2023-18-6-98-108;
17. Sajeed, S., Chaiwongkhot, P., Huang, A. et al. An approach for security evaluation and certification of a complete quantum communication system. Sci Rep 11, 5110 (2021). <https://doi.org/10.1038/s41598-021-84139-3>;
18. Математическая модель квантового генератора случайных чисел на основе флуктуации вакуума / А. А. Гайдаш, Р. К. Гончаров, А. В. Козубов, П. В. Яковлев // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. – 2024. – Т. 20, № 2. – С. 136-153. – DOI 10.21638/spbu10.2024.202. – EDN KBUVNP;
19. Уязвимости систем квантовых коммуникаций в видимом диапазоне длин волн / Б. А. Наседкин, А. О. Исмагилов, В. В. Чистяков [и др.] // Невская фотоника-2023 : Всероссийская научная конференция с международным участием сборник научных трудов, Санкт-Петербург, 09–13 октября 2023 года. – Санкт-Петербург: Национальный исследовательский университет ИТМО, 2023. – С. 186. – EDN PSXUMZ;
20. Канатъев К.Н., Нурмагомедов М.Д., Гребенщиков А.А., Каравцев Н.А., Станолевич В.С. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху // ИННОВАЦИИ И ИНВЕСТИЦИИ. - 2023. - №10. - С. 211-214;
21. Д. Н. Колегов, Ю. Р. Халниязова, “Использование российских криптографических алгоритмов в протоколе безопасности сетевого уровня WireGuard”, ПДМ. Приложение, 2021, № 14, 81–84;

© В. С. Пустовит, 2026